Chapter 1

Introduction to Blockchain Technologies

Experts in the technology and financial sectors consider blockchain technology to be revolutionary. Your role, as a solutions engineer, presales engineer, or customer-facing sales professional, may require knowledge now or later in your career to sell blockchain technology solutions. It is important to appreciate how the blockchain is changing the world and how you as a value-added reseller (VAR)/vendor/integrator or even a professional services organization can participate in the blockchain revolution.

Blockchains are not a product to sell, such as a server, a data storage array, or a network router. Blockchains are an "exercise in development" to essentially sell, service, and develop a blockchain-focused solution. Blockchains can certainly "enable" products and, as a result it can be complex to design, implement, and develop applications around. Sometimes legacy applications can be extended, which is a common design and integration approach that enterprises should consider. Essentially, the technology behind blockchains is simple, but the implementation of the technology is where it gets more complex. The goal of this chapter is to break down blockchain technology for a sales-driven and technically focused audience.

This chapter discusses the technical merits of blockchain technology in a simple manner with direct correlations to how it applies to business.

IN THIS CHAPTER, YOU WILL LEARN THE FOLLOWING ABOUT BLOCKCHAINS:

- What a blockchain is and how to define a blockchain
- The history of the blockchain and why the history is important to appreciate
- How blockchains compare to other enterprise technology platforms
- What blockchain transactions are and how they provide value to the enterprise
- What a trustless model is compared to a trust model
- Why the blockchain is considered revolutionary
- Types of blockchain platforms

Architecting Enterprise Blockchain Solutions, First Edition. Joseph Holbrook.

What Is a Blockchain?

Blockchains have been considered a disruptive technology and the start of what has been coined the Web 3.0 generation. Web 3.0 is the next technology front on the Web where many devices are interconnected (called the Internet of Things) and used with technologies such as automated intelligence. Blockchain technology has significant ramifications for specific industries that perform fiduciary or intermediary duties, as you will see in this chapter and throughout the book.

To be clear, there is a significant amount of confusion about what a blockchain really is, how it creates value, and whether it's a cryptocurrency. Another issue is that blockchains have very different use cases; some blockchains are only for cryptocurrencies, while others do not support cryptocurrencies.

To gather an understanding of where blockchains and cryptocurrencies came from, it is important to appreciate Bitcoin. Bitcoin was the real start of blockchain technology because it provided a use case to society. Satoshi Nakamoto, in his 2008 paper "Bitcoin: A Peer-to-Peer Electronic Cash System," created the concept of the blockchain.

Nakamoto's paper had some detailed approaches to how a blockchain should be purposed for the benefit of the masses.

- A blockchain should be a trustless online payment network that is based on peer-to-peer (P2P) versions of electronic cash. The network is a robust node structure that works together with little coordination.
- A blockchain should alleviate the challenge of double spending, where funds can be over drafted and therefore lost to the wallet holder.
- A blockchain should implement the proof-of-work consensus method that rewards nodes that participate in the creation blocks (miners). The miners are rewarded for participation through an incentive approach, and this encourages miners to be honest.
- A blockchain should simplify privacy through a trustless system that removes intermediaries and introduces the use of anonymous public keys.

If you read Nakamoto's paper, you will likely conclude that enterprise permissioned blockchains were not in Nakamoto's vision at the time. The realization of this requirement for enterprises was not introduced for years after Bitcoin became mainstream.

One of the main challenges in the blockchain arena is how to answer the question, "What is a blockchain?" If you ask 10 different blockchain experts, you will get 10 different answers. The following are just some of the definitions of what a blockchain is:

- A blockchain is a shared distributed ledger or data structure.
- A blockchain is a distributed root of trust on a distributed ledger.
- A blockchain is a digital ledger in which transactions made in Bitcoin or another cryptocurrency are recorded chronologically and publicly.
- A blockchain is a type of distributed ledger for maintaining a permanent and tamper-proof record of transactional data.
- Blockchain technology is a distributed ledger technology that uses a distributed, decentralized, shared, and reciprocal ledger, and it may be public or private, permissioned or permissionless, and driven by tokenized crypto economics or token-less.

These definitions all focus on a ledger—specifically, a distributed ledger. A *ledger* is essentially a written or computerized record of all the transactions a business has completed. A *distributed ledger* is a database that is consensually shared and synchronized across networks that are spread across multiple sites, institutions, or geographies.

My Approach to the Definition

My approach to defining blockchains is somewhat varied from what other blockchain evangelists will provide. I believe that there is no one correct definition that will provide a realistic understanding of the blockchain technology to everyone. This book presents several blockchain definitions that will vary depending on the audience.

My experience as a presales engineer has taught me that different types of audiences have different levels of interest in how technology works. For example, one would not expect an attorney to understand information technology the same way a SQL developer would. Both a developer and an attorney have different training and for that matter think differently.

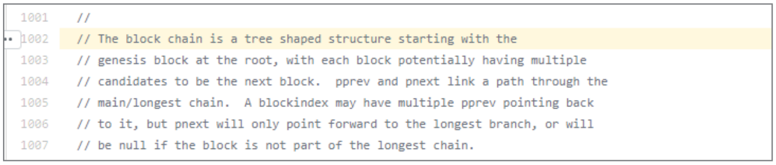
My definitions of a blockchain focus on the following audiences:

- Technical, which includes IT staff, developers, and other technical stakeholders.
- Business, which are generally IT directors, C-level suite members, and stakeholders of financial organizations.
- Legal, which is generally any compliance-related auditors, corporate counsel, or other types of attorneys. Legal would entail government regulators, as well, depending on your use case.

Technical Audience

Figure 1.1 shows the first definition of a blockchain from Nakamoto's 2008 paper. This is a definition for a technical audience. Satoshi's blockchain definition is somewhat complex, but in simple terms he is describing the chaining of blocks. From a historical and technical perspective, reviewing Nakamoto's definition should provide insight into his thinking when creating Bitcoin.

FIGURE 1.1
Nakamoto's original blockchain definition



```
//
// The block chain is a tree shaped structure starting with the
// genesis block at the root, with each block potentially having multiple
// candidates to be the next block.  pprev and pnext link a path through the
// main/longest chain.  A blockindex may have multiple pprev pointing back
// to it, but pnext will only point forward to the longest branch, or will
// be null if the block is not part of the longest chain.
```

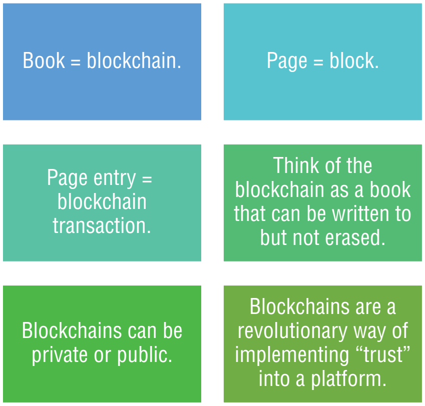
Comparing the definition in Figure 1.1 to the other widely used definitions listed earlier, you can see that there are significant differences. My point here is that if you're confused about what a blockchain is, you are not alone. The IT industry has done a poor job of providing a standard definition.

Business Audience

During discussions with customers (or students), I like to compare blockchains to a hard-copy notebook. In essence, a blockchain is a ledger, albeit a distributed data structure and immutable ledger. When you write in a notebook, each entry will take up one line. Think of a blockchain as a notebook where entries will be written but cannot be erased.

Figure 1.2 compares the properties of a blockchain ledger to a notebook. Comparing a blockchain to a notebook is a simplistic approach, of course. A page is compared to a block on a blockchain and a page entry is actually a blockchain transaction. Blockchains are about implementing trust.

Figure 1.2
Comparing a blockchain to a notebook



Book = blockchain.

Page = block.

Page entry = blockchain transaction.

Think of the blockchain as a book that can be written to but not erased.

Blockchains can be private or public.

Blockchains are a revolutionary way of implementing "trust" into a platform.

When it comes to comparing a blockchain to a notebook, it would be accurate to assume that not all blockchains are created equal, just as not all notebooks are created equal. For example, Ethereum handles transactions somewhat differently from Hyperledger Fabric when ordering and validation are considered. When you consider a notebook, you know that some notebooks have lines, some do not have lines, and perhaps some have boxes.

Blockchains are all about trust in the technology and removing third parties or intermediaries. A blockchain is a globally shared data structure, with a transactional backend database that is cryptographically secure. Everyone can read entries in the database just by participating in the network. If you want to change something in the database, you have to create a so-called *transaction*, which has to be accepted by all the others in the blockchain. The word *transaction* implies that the change you want to make (assume you want to change two values at the same time) is either not done at all or completely applied.

Blockchains are not built from any new transformative technology but are built from a unique syncing of three existing technologies: peer-to-peer networks, cryptography, and programs (known as *smart contracts* in the world of blockchains).

Another factor to consider is the cost. Even the cost of implementing these technologies is near zero when you consider there are numerous open source projects available. Blockchains are not complex technology when viewed holistically, but the complexity can be introduced when integrating these systems into the enterprise.

Let's compare Bitcoin to a blockchain and understand how these terms come together. Bitcoin is an unregulated digital currency that uses the blockchain technology as its transaction ledger. A blockchain is the platform for most cryptocurrencies and is the "enabler" for Bitcoin; Bitcoin is the application (cryptocurrency) that is being "enabled." Think of it like the blockchain is the train track, and Bitcoin is the train. Or, the blockchain is the telephone network, and Bitcoin is the phone.

At a high level, Bitcoin transactions work as follows. A sender wants to transfer funds to a recipient. The transaction is represented online as a block. The block is broadcast to every network participant. The network participants review the block, and if approved, it is added to the blockchain. Finally, the money moves from the sender to the recipient.

Legal Audience

Lawmakers have even gotten into the arena of defining the term *blockchain*. A pair of U.S. representatives, California Democrat Doris Matsui and Kentucky Republican Brett Guthrie, introduced H.R. 6913, "Blockchain Promotion Act of 2018," to bring stakeholders together to develop a common definition of *blockchain*. The bill also recommends opportunities to promote new innovations. See `https://www.congress.gov/bill/115th-congress/house-bill/6913`.

In addition, the State of California recently defined what a blockchain and smart contract are. See `http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB2658`.

Three Definitions of Blockchain

The blockchain technology has clearly been transformational in the financial, logistics, and government sectors. The following definitions are aligned to the specific audiences of technical, business, and legal that I'll be mentioning throughout this book:

- **Technical definition**—A globally shared and secured data structure that maintains a transactional backend database that is immutable.
- **Business definition**—A business network that is used between peers to exchange value. Value can be currencies, tracking information, or anything that interested parties require to be maintained on the blockchain ledger.
- **Legal definition—**A corruption-resistant string of ledger entries shared over a network by multiple parties not requiring a centralized intermediary to present and validate transactions.

As a customer-facing professional, you must define the right blockchain jargon to the right audience. Not everyone is going to be technical nor is everyone just concerned about the business aspects. When you're discussing blockchain with your customers, try to appreciate the role that they are in and cater the definition to them. This will likely facilitate understanding around the blockchain technology.

History of Blockchains

As previously mentioned, the first known blockchain solution was Bitcoin. Bitcoin's main innovation was bringing cryptocurrency to the world. *Cryptocurrency* allows people to transfer value without the centralized high costs and improves on the slow transfer times and other challenges associated with legacy banking systems, such as SWIFT. SWIFT is a proprietary global financial network for its membership of banking institutions.

Bitcoin was essentially an experiment that started a march toward a decentralized payment approach that left banks out of the transaction. Bitcoin was devised during the great financial recession of 2007 and 2008. Removing the banks provides benefits such as decentralization, faster transfer, and lower risk because one controller is not performing payment processing centrally. Decentralization, P2P, and cryptography are at the core of Bitcoin's success around the world. In addition, its effects will certainly change the payment and remittance market for the better by lowering remittance costs for consumers.

Besides bringing cryptocurrency to the masses, Bitcoin's second innovation was the platform it runs on, which is the blockchain or distributed ledger. For enterprises, the blockchain disruption will take place because it provides one or more capabilities around compliance, cost efficiencies, or even transparent transactions for the customer base. The benefits for the enterprise in some industry verticals could be multifold such as what we are witnessing in the logistics sector around blockchain acceptance. I believe blockchain is the next great technology that will enable more financial engineering for companies just as cloud computing or offshoring has historically.

Cloud computing is a centralized form of data center management that is totally dependent on cloud providers performing accordingly. Trust is clearly expected for this relationship to work around data security, availability, and support. In Chapter 7, "Blockchain as a Service," I discuss more about cloud computing and how to deploy a blockchain on various providers.

Cloud computing has significant benefits to the user and has leveled the playing field between large Fortune 100 companies and small startups. Smaller companies can utilize cloud services at the same cost that a large company can. The cloud has also allowed companies to reduce overhead, reduce investments in infrastructure, and indirectly increase executive compensation along with corporate earnings.

In fact, a company's most important asset is sometimes not its employees but rather its data. Therefore, if companies are going to let another company control access to their data to save money, then those cloud companies, in my experience, will get into blockchain because of the ability to utilize a consortium and share costs. Blockchain as a service (BaaS) has already made significant headlines and has major backing by all the major cloud providers. The business model for many organizations follows the monetization of the collection, mining, and distribution of data. It's really all about the data and creating revenue from that data at the lowest cost historically.

This business model could also be enhanced through the use of consortiums. *Consortiums* are agreements that are made between organizations to work together and collaborate. Consortiums are communities of people or organizations with the same use case for a service.

Generally, these consortiums provide some benefits such as increased cooperation, standardization, integration ease, and even financial efficiency.

The consortium approach that is currently used in some of the most successful blockchain implementations can provide significant ROI, TCO, and other financial benefits to the member companies. If your customer has, for example, numerous points of overhead, then consider talking about blockchain use cases that they can relate to. Customers who have intermediaries such as transfer agents, customs inspectors, attorneys, and accountants are all spectacular potential targets for blockchain technology. In Chapter 6, "Enterprise Blockchain Economics," I cover the many benefits of blockchain economics such as consortiums.

The reality is that companies that have been immensely successful are investing millions and even hundreds of millions into blockchain technology. They are not doing it for "goodwill" but as a means of survival. It's all about the changing business environment, which is becoming globally centralized as a result of economics.

The list of companies that are investing in blockchain technology is a "who's who" of the Fortune 500, and I would not bet against them based on my experience. They see potential in the technology from several angles such as security, privacy, financial, and even legal requirements.

NOTE "I think this is the beginning of the point where now these technologies are becoming mainstream enough, people understand it enough, that they can begin to deploy it. I expect this to grow pretty rapidly in the next couple of years." —Mark Russinovich, CTO MS Azure (`https://www.investors.com/news/blockchain-mainstream-industry-applications-microsoft-azure-cto/`)

Historically, some consistent factors of blockchains that have had a major impact on the enterprise acceptance of blockchain technology are as follows:

- Autonomous innovations such as smart contracts and decentralized applications (dapps) have contributed to the impact that enterprises can have through the efficiencies that can be attained.
- Cost-effective solutions have reduced intermediary costs or overhead costs such as reducing the number of intermediaries or all intermediaries for an enterprise.
- Transactions costs for payment remittance, such as on interbank transfers or settlements, have greatly affected profitability in companies, especially in the financial sector.
- Providing transparency in supply chains has enabled consumers to understand the sourcing of their buying choices and the chain of custody from source to market.
- Permissioned blockchains can scale and provide enterprise-level security.
- Perhaps the most important innovation is the smart contract. A *smart contract* is essentially computer code that executes a specific task and when properly developed as part of a distributed application can provide significant efficiencies, compliance, and performance. (During the course of the book, I will discuss smart contracts from both a business perspective and a technical perspective.)

It is important to understand how a technology has evolved, how it has changed over time and in structure, or how it provides value to organizations. I will now give you an idea of how blockchain really got started from an even older historical perspective.

The Byzantine Generals Problem (BGP) is considered a classic problem of computing. To explain the military metaphor, BGP can occur when a number of generals (from the same army or even allies) have surrounded a walled castle or a city on all its sides. The balance of power is such that all generals must attack at the same time in order to take the city.

In computer science, this is referred to as a *distributed node network*. It is critical to understand how a centralized system compares to a decentralized system to understand why Bitcoin came about. For example, what happens when a distributed system gets out of sync? How does the system handle an out-of-sync status?

In a centralized network, there is one central authority or server. The other participating nodes on the network act like clients or entities that accept messages and perform tasks.

In a decentralized network, there can be multiple servers that receive messages from one centralized server. The individual nodes are connected to the secondary servers. In another form of a decentralized network, all servers are of "equal" responsibility in the network, with no centralized server or master/slave relationship. In many cases, a decentralized network is considered a subset of a distributed network in many cases.

In distributed systems, there is no server with a centralized authority. Each node on the network is connected to every other node and has the same authority and processing capacity, which is shared. This is similar to a blockchain.

Figure 1.3 compares centralized systems, decentralized systems, and distributed systems with highlighted node connections.

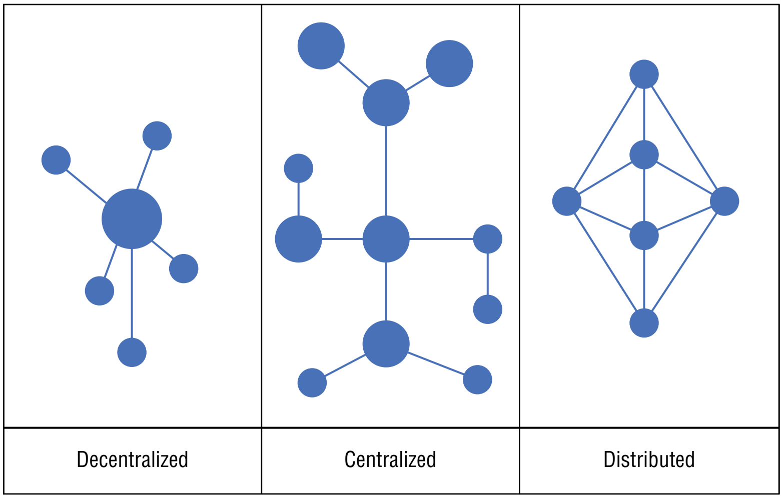


FIGURE 1.3 Comparing networked systems

Blockchains by definition are not centralized systems, although some blockchains have centralized properties over decentralized or distributed properties. In Nakamoto's 2008 paper detailing Bitcoin, he outlined a solution to the nature of distributed nodes. (You can compare nodes to generals in our Byzantine Generals Problem.)

The industry really started after Nakamoto came out with Bitcoin in 2009. However, the enterprise environment did not really get started until 2015 with permissioned blockchains. (Permissioned blockchains are generally referred to as *enterprise blockchains*.) So, the blockchain technology is no more than 10 years old at the time of this writing, and enterprise blockchains such as Hyperledger (covered in Chapter 2, "Enterprise Blockchains: Hyperledger, R3 Corda, and Ethereum, Quorum") are less than 5 years old!

NOTE The following are the release dates for popular blockchains:

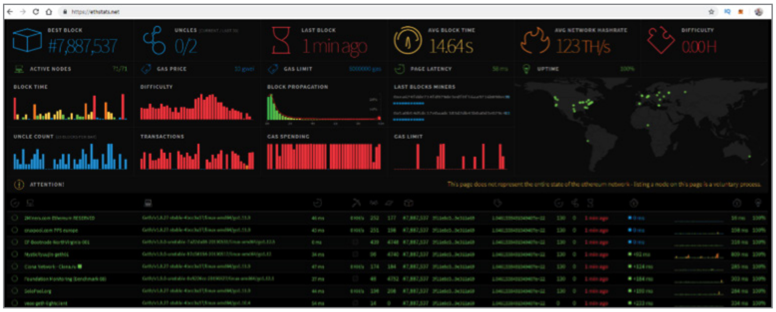
- 2009—Bitcoin
- 2015—Ethereum
- 2015—Hyperledger
- 2017—R3 Corda

Blockchain vs. Traditional Database

It is important to understand how the distributed blockchain ledger differs from a traditional database. A distributed ledger is a database that is stored and updated independently by each node in the blockchain. Every node essentially maintains a copy of the blockchain. For example, in the Ethereum blockchain network, there were more than 16,000 nodes at the time of writing. In the Bitcoin blockchain network, there are more than 7,000 nodes at the time of writing. Why is this important? Every node that is online has a current copy of the working blockchain. If you lose a few nodes, it's no big deal since there are thousands of other nodes that maintain a copy. In the Ethereum network, when a transaction is written to the ledger, it also is written to more than 1,600 other nodes. Does a centralized database maintain 1,600 copies of its database? Of course not.

Figure 1.4 shows the vast Ethereum network with the Etherstats.io service. You can view many different data points of the Ethereum blockchain, as Etherstats provides transparency into the Ethereum blockchain.

FIGURE 1.4
Ethereum network
Etherstats.io



This page does not represent the entire state of the ethereum network - listing a node on this page is a voluntary process.

An enterprise would likely be interested in using the Ethereum virtual machine (EVM) for running its off-chain smart contracts or for a token platform that is being built for a distributed application known as a *dapp*. It would then look at the Ethereum Explorer referenced in Figure 1.4 and review the hash rate or the gas numbers.

The Ethereum ledger is also great for keeping track of transactions and providing transparency to your customer base. In Chapter 2, I will cover Ethereum in much more detail and explain why enterprises are interested in Ethereum.

What is the biggest difference between a database and distributed ledger or a blockchain? Well, the decentralized and distributed nature of the blockchain is what makes blockchain ledgers unique compared to traditional databases such as SQL. Databases and ledgers are generally centralized, meaning that there is a centralized administrator or centralized node structure that can create, delete, modify, or update the database. Some common databases include Microsoft SQL, Oracle PL/SQL, and IBM DB2.

In the traditional database world, objects are used as a data structure, and these objects are *mutable*, meaning that they are able to be modified or deleted. In a blockchain, an object is not modifiable after it has been created, and therefore it is considered *immutable*.

Distribution of Trust

The primary solution that blockchain technologies really provide as compared to a traditional database is around the distribution of trust. In a traditional database, the trust is centralized; in a blockchain, the trust is distributed among nodes of the blockchain.

Distribution of trust means that not only does one blockchain node have a copy but every blockchain node maintains a copy. For example, if there are 1,000 nodes in an enterprise blockchain, then at its truest form the blockchain acts as a "truth agent." The likelihood that 1,000 nodes could be hacked or controlled is statistically impossible with blockchains that are true blockchains since the ledger is a distributed ledger.

Consensus and Trust

Blockchain ledgers are decentralized, distributed, and immutable. This is critical to trust, which is built on the fact that they can't be modified or deleted.

Consensus is an approach that is utilized on a distributed ledger network where all the network nodes maintain a copy of the ledger. The ledger is used to come to an agreement on whether a transaction is valid.

For example, in Ethereum, the ledger, which is distributed among nodes in more than 100 countries at the time of writing, is used for blockchain transactions. This ledger is distributed globally and can be accessed from anywhere with an Internet connection. To access the ledger, you would need the public keys that Ethereum uses for authentication.

Figure 1.5 provides more insight into how an Ethereum transaction occurs at a high level. Jamie is being sent $100. This amount will be deducted in ether from the sender's wallet and deposited into the receiver's wallet.

Remember, the nodes in the blockchain network in most permissionless (enterprise) blockchains have a copy of the whole blockchain. This means that every single node on the network processes every transaction that occurs, and there are multiple copies of that ledger. There is now consensus (an agreement) that this transaction is valid.

Summary of Differences Between Ledgers and Traditional Databases

You now know that blockchains have ledgers, and these ledgers are different from traditional databases in the following ways:

- Legacy architectures in databases are basically centralized repositories of managed data. This data, though, is usually structured and controlled centrally. Blockchains are decentralized and distributed between nodes on the blockchain network. Data is managed by consensus and not centrally controlled.
- SQL or NoSQL are common legacy database applications. SQL is the most widely used database. Blockchains do not use SQL or relational database structures.
- Whether centralized or distributed, traditional databases use client-server network architecture. Blockchains are decentralized and distributed data structures.
- Database processing speed is referenced as transactions per second (TPS), and legacy databases are much quicker in most cases compared to blockchains when it comes to TPS.
- Control of the database remains with a designated authority in a legacy database, whereas in a blockchain there is no centralized authority.

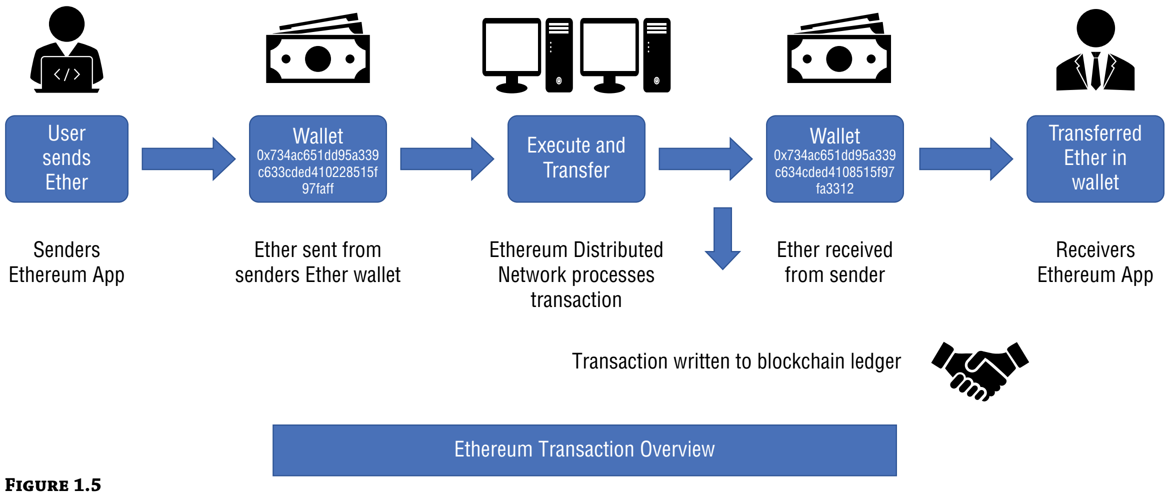

User sends Ether
Wallet 0x734ac651dd95a339c633cded410228515f97faff
Execute and Transfer
Wallet 0x734ac651dd95a339c634cded4108515f97fa3312
Transferred Ether in wallet
Senders Ethereum App
Ether sent from senders Ether wallet
Ethereum Distributed Network processes transaction
Ether received from sender
Receivers Ethereum App
Transaction written to blockchain ledger
Ethereum Transaction Overview

Figure 1.5
Ethereum transaction

- Data can be modified or even deleted in a legacy database, but in a blockchain this cannot occur since a blockchain is immutable.
- Databases conform to the principle of CRUD (create, read, update, and delete), and blockchains conform to the principle of CR (create and read only).

Cap Theorem

The CAP theorem, also known as Brewer's theorem, was introduced by Eric Brewer in 1998, and provides significant insight into the problem of distributed systems had around maintaining consistency, availability, and partition tolerance and was based on factual evidence at the time.

In 2002, the CAP theorem was proven as a theorem by Seth Gilbert and Nancy Lynch, respectively. The CAP theorem states that any distributed system cannot have consistency, availability, and partition tolerance simultaneously. Another way to look at the CAP theorem is that it is a tool that can be used to make system designers aware of the possible property trade-offs while designing networked data stores.

According to the CAP theorem, there must be some property that is reduced to provide for the other two properties. The properties in the CAP theorem are as follows:

- *Consistency* means all networked nodes in a distributed system have the same view.
- *Availability* means that the nodes in the system are available, meaning they are online and accepting requests.
- *Partition tolerance* means that if a node goes down, other nodes are fine.

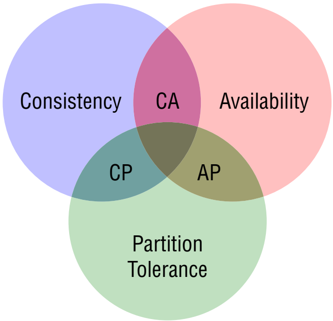
Note that it has been proven that a distributed system cannot have consistency, availability, and partition tolerance simultaneously. Essentially, you cannot have them all in a distributed system, and when designing an enterprise service—whether or not the service is a blockchain—you will need to choose what properties are more important to provide to your customer.

The CAP theorem categorizes systems into three categories: consistent partitioned (CP), consistent and available (CA), or available and partition tolerant (AP).

When considering a distributed ledger, realize that latency will come into the picture to some degree and needs to be designed around. Ledgers that are distributed over a local data center will, of course, perform differently than ledgers that are distributed on a cloud provider's regions and zones. Latency can make or break an application and the users' experience with the application.

Figure 1.6 shows how the CAP theorem is structured. Notice the overlap between the three properties. These three properties in a blockchain will never be perfectly aligned.

FIGURE 1.6
Cap theorem



For example, it is important to appreciate the three CAP theorem as applied to your blockchain network.

- Consistency is achieved only if all nodes have the same shared state, meaning that they have the same up-to-date copy of the data.
- Availability is achieved only if all nodes are up and running and are responding to transaction requests for the latest copy of data on the ledger.
- Partition tolerance is achieved between two nodes or more only if they are able to communicate with each other. Communication on any network is subject to latency, jitter, and TCP protocol challenges.

Consistency is achieved in blockchain networks using consensus algorithms that ensure all nodes have the same copy of the data. This form of consistency is similar to replication, but in the IT world we would call this *state machine replication*. The blockchain is a means for achieving state machine replication, and this can be accomplished in several ways based of course on the blockchain.

There are two types of faults that a blockchain node can experience on a distributed network.

- The first type of fault is called a *fail-stop fault*. This type of fault occurs when a node has merely crashed. Fail-stop faults are the easier ones to deal with of the two fault types. The Paxos protocol can be used to resolve this concern. (Paxos is a protocol suite that solves consensus challenges in a network of inconsistent nodes.) Basically, networks have challenges such as latency that can greatly worsen the more a network is distributed.
- The second type of fault is one where the faulty node exhibits malicious or inconsistent behavior arbitrarily. This fault is difficult to handle since it can create arbitrary results.

Consistency on the blockchain is not achieved simultaneously with partition tolerance and availability, but it is achieved over time. Since the consistency is achieved over time and is not immediate, it is called *eventual consistency*. Distributed networks are slow, and maintaining this consistency needs to be addressed.

The concept of mining was introduced in Bitcoin for this purpose to maintain the consistency of the blockchain network. *Mining* is a compute-intensive process that facilitates the achievement of consensus by using the proof-of-work (PoW) consensus algorithm.

Mining can also be defined as a process that is used to add more blocks to the blockchain as a result of the consensus method. PoW and other common consensus methods are covered in detail in Chapter 4, "Understanding Enterprise Blockchain Consensus."

Common Properties of Permissionless Blockchains

Permissionless blockchains are blockchains that open to the public and have no permissioning meaning the users do not need authorization to use the platform. The right customer may very well be a business-to-consumer model where the customer may want visibility into a special order such as a custom necklace that is being sourced overseas and is moving thru the logistical processes which would provide the customer "visibility" or in blockchain what we would call "transparency".

Table 1.1 shows the more commonly referenced features of what a blockchain provides. As you can see, there are a handful of common features that blockchain provides.

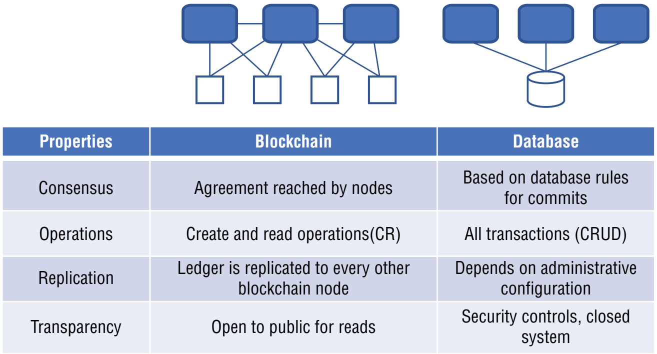
TABLE 1.1: Common Blockchain Features

FEATURE	NOTES
Global computer network	Distributed nodes, with no centralized control of nodes.
Ubiquitous access	Can access the resources with only an Internet connection from anywhere.
Censorship and tamper-proof ledger	No entity can modify or delete data, which makes the blockchain immutable. Immutability provides data compliance since it cannot be deleted or modified.
Open source	Uses programming languages that are portable, which allows ease of development.
Compliance	Comes with smart contracts that are validated. The blockchain ledger also is verified by audits.
Multiple users	No limitations to who can join the blockchain, and the accounts scale.
Trust	Trust in the code (smart contracts), which means that users place trust in the blockchain technology.
Guarantees	Atomicity, synchrony, and provenance.

Blockchain and traditional databases have properties that are similar to each other but also have properties that are not similar to each other. For example, both a blockchain and a traditional database replicate data. However, the way replication is initiated, achieved, and handled is actually very different from a comparative standpoint.

Perhaps the most important difference is how blockchains and databases handle operations on the ledger. Blockchains will only insert operations to the ledger, meaning that the transaction is one-way. In a database, the transactions can be any transaction from an insert or delete operation, meaning create, update, or delete.

Figure 1.7 compares properties of a blockchain to a traditional database: operations, replication, consensus, and invariants. When comparing a database to a blockchain, the property difference is significant.



Properties	Blockchain	Database
Consensus	Agreement reached by nodes	Based on database rules for commits
Operations	Create and read operations(CR)	All transactions (CRUD)
Replication	Ledger is replicated to every other blockchain node	Depends on administrative configuration
Transparency	Open to public for reads	Security controls, closed system

FIGURE 1.7 Blockchain vs. traditional database comparison

It is important to note that the blockchain allows for two specific functions only in its truest implementation.

- The validation of a transaction
- The writing of a new transaction

Notice that modifying data and deleting data are not functions blockchains support. Blockchains append to the blockchain, and that is the only function that should be supported. Blockchains are stateful programs and thus have some mechanism to keep track of and update state. They maintain the past and thus remember previous transactions that may affect the current transaction. The term used in blockchain transactions is *append*. (I will be covering this in detail throughout the book.)

Why the Blockchain Is Considered Revolutionary

During the course of the last 100 years or so, the advancement of life-changing technologies has been dramatic. It is also reasonable to say that the potential of newer technologies such as artificial intelligence, machine learning, and blockchains will all impact our lives significantly. Technology often can be revolutionary, and the blockchain technology looks like it will be one of those.

The blockchain technology is revolutionary in several ways, as listed here:

- The blockchain technology is a syncing of technologies that now make sense to implement strategically.
- Trust is at the center of blockchain technology and through the use of consensus removes intermediaries from the network and thus creates new efficiencies that companies can really benefit from, such as providing transparency, a root of trust, a reduction in labor costs, and numerous other benefits.
- The blockchain technology in its true sense, as specified by Nakamoto, is a "tamperproof public ledger of value." The Bitcoin platform enabled citizens of the world to make transactions without the need of intermediaries.

The blockchain technology is disruptive to the status quo since legacy applications and business processes are being phased out with blockchain applications.

Blockchain is a platform with numerous use cases for enterprises. The number and quality of organizations investing in blockchain testing, implementation, and production specifications is impressive.

Blockchain Principles

Clearly, the principles implicit in blockchain technology have lent themselves to the redesign of software, businesses, organizations, and even governments. The principles of blockchain have renewed trust in users in an era of digital economics and intrinsically fair social systems.

- Trust is provided through the implementation of technology. The technology used in a blockchain for establishing trust is provided through encryption and code which validates the transaction requirements and will determine if a transaction is securely accepted or rejected.

- Integrity is provided through the blockchain network where there is no centralized authority or failure point, and every transaction is recorded.
- Incentives are distributed to all stakeholders to the participants that produce blocks, and these participants are called *miners*.
- A blockchain is decentralized, meaning that the data is distributed among thousands of nodes and there is no centralized point of control.
- Privacy means that users are in control of how the data is handled. There is no requirement for compliance such as know your customer (KYC), for example.
- Equal access/inclusion is in effect in the manner that everyone in the world should have the ability to participate in the blockchain network.

Trust or Trustless

Blockchains do not actually eliminate trust; rather, they minimize the amount of trust required from any single actor/participant on the network. They do this by distributing trust among different actors in the system via an economic game that incentivizes actors to cooperate within the rules defined by the protocol. The economic incentives are presented for participating in the permissionless blockchains such as Ethereum or Bitcoin; miners produce blocks and obtain rewards for mining.

Blockchains define a secure communication protocol that allows two individuals to transact with one another in a "peer-to-peer" manner over the Internet. This means there are no intermediaries facilitating transactions.

When you digitally transfer value from one account (wallet) to another account (wallet) on the blockchain, you're trusting the underlying blockchain network to enable that transfer and to ensure the sender's authenticity along with the cryptocurrency's validity. *Authenticity* means that the sender is who they present themselves to be electronically via public key encryption usually implemented through certificates and keys. *Validity* means that the sender has the correct wallet and has funds in that wallet to actually send the correct amount of funds.

For example, in the centralized approach, you may need to use Western Union to send funds from the United States to Peru. The cost to do this as well as the time to perform this transfer could be substantial in some cases; it could be a few hours, a few days, or longer. In addition, the transfer fees can be 10 times or more than using cryptocurrencies on a blockchain network.

Basically, you are "trusting" the intermediary to validate the transaction, send the transaction, and confirm the transaction has completed. You might use this service because you expect the transfer to be valid and authentic since the intermediary is performing a fiduciary responsibility. People clearly trust banks, nonbanks such as PayPal, and other entities such as Western Union to send funds to people who request them. However, that trust can come at a cost, whether financial or otherwise.

Trustless is generally used to describe "distribution of trust" where the trust is not placed in a centralized concentration but is actually distributed in a decentralized manner to all the participants in the blockchain.

With blockchain consensus methods, this approach allows participants to share digitally distributed "truth" that is stored on a distributed ledger that is not centralized. The truth could be a list of transactions, voucher IDs, customer addresses, or any assets or information that can be written to a blockchain.

Trust Blockchains

Trust is at the center of all blockchains whether permissioned or permissionless, albeit they approach trust differently.

A blockchain is a truth machine because of the implementation of the technology used, and this implementation of the ledger maintains the truth since the ledger is an immutable record of trust.

In its most basic form, a blockchain is an immutable record of transactions. These transactions can be any type such as movement of money, products, or even services. Blockchains are designed to store information in a way that makes it virtually impossible to add, remove, or change data without being detected by other users.

When considering blockchain technology, it is imperative to understand how trust is established with blockchains. The following list highlights some important considerations:

- The blockchain technology is about storing some kind of data—for example, transactions such as in the case of the Bitcoin blockchain or tokens in Ethereum. The platform is trusted to perform these transactions because of the code and encryption utilized. Trust is distributed between the blockchain nodes on the Ethereum platform.
- The blockchain technology is essentially transferring trust from an intermediary to technology (software code).
- Storing data in the blockchain happens through cryptographic functions such as certificates and keys.
- Private keys/public keys are used to secure transactional data written to the ledger through Public Key Infrastructure (PKI).

When considering the reasons why users can trust a blockchain, there are two main considerations.

- All transaction data on a blockchain is assumed to be trustworthy because the blockchain protocols are enforced and encryption is used.
- The blockchain users base this trust in a blockchain on the following:
  - The blockchain data has not been tampered with and is being managed by nodes producing blocks on the blockchain.
  - The blockchain ledger that contains the data is immutable and therefore cannot be deleted, modified, or moved.

Trust is at the epicenter of how blockchains function and the value it creates for enterprises and users.

Trustless Blockchains

When considering blockchains, the model that is used is considered a trustless model where trust is transferred from an intermediary to technology.

A trustless model does not require "trust" in order to safely interact and transact as trust is considered inherent in the technology platform. A trustless blockchain, in reality, is a transfer of trust to the blockchain technology from humans in centralized organizations (banks, governments, corporations).

Blockchains are built on the premise that transparent code (smart contracts) essentially removes the need for intermediaries. Smart contracts can essentially reduce the need for accountants, lawyers, bankers, and so on. Essentially, trust is transformed. "Trustless" in blockchain essentially creates the trust by default, which means when users utilize a blockchain, they are "trusting" the technology to perform as it should.

Transparency and Blockchain

The blockchain technology is decentralizing information dissemination and providing transparency that has never been seen before. Blockchain's main focus on ledger management and immutable records makes it a perfect technology candidate for the decentralized tracking of resources, which could provide transparency to an enterprise customer purchasing something of value, for example.

Consumers increasingly require more transparency into the services and products they purchase. The following list are some areas of focus where the blockchain industry is seeing significant demand for use cases, proof of concepts, and implementations:

- Food supply traceability
- Labor credential validation
- Logistics and supply chains
- Customs compliance
- Corporate governance

The transparency of a blockchain comes from the openness of the blockchain transactions viewable to anyone. This transparency, in Ethereum, for example, is accomplished using a blockchain explorer such as Etherstats. A blockchain explorer provides insight into the transactions on a blockchain. For example, in Ethereum your wallet address is what links the transaction to the blockchain user. There is no identifying information, such as name or address of the wallet holder.

The transparency provides insight into how many Ether was sent and received, to what wallet address, and other critical information such as the block height or transaction ID. However, it is important to note that transparency does not provide an identify of who actually sent the ether.

For example, this blockchain explorer translates the ledger and provides some privacy in the sense that a wallet address is displayed (transparency) but the owner of the wallet is not provided publicly (privacy).

Pseudonymous is used to reference a blockchain transaction, where the sender and receiver are not directly identified.

Here are some examples of blockchain applications that provide this transparency:

- Ledgers stored in the blockchain make it easier to track ownership and liability during transit, limiting liability protecting practitioners and pharmacists who administer drugs to patients
- Blockchain technology can be applied to several different aspects of the healthcare space such as managing electronic health records (EHRs), which will be used for validating patient data, and even tracking research methods used to make safer drugs across clinical trials.

- The blockchain technology in the logistics industry, for example, has numerous in-production use cases. One of the more widely publicized is focused in the jewelry industry, which has traditionally been known for high levels of fraud, child labor issues, false metal mining, and a clear lack of transparency.
- A precious metals consortium with IBM has established a blockchain initiative to bring transparency to the consumer. For example, consumers can validate that their purchases are ethically sourced from sustainable resources without the involvement of child labor.

Some common consumer advantages of transparency in blockchain technology include the following:

- Blockchains are open for viewing and validating transactions, meaning that they are transparent for customers, consortium members, and the enterprises.
- Blockchains provide a pseudonymous feature for participants that allows the transactions to be transparent but the users to be unidentified by direct means such as name or address. A wallet address is used, but the name of the wallet owner is not clarified.
- Participants share the same ledger and establish a shared consensus service that can be referenced by the stakeholders.
- Blockchains provide integrity opportunities for businesses that provide services in a logistic blockchain. Integrity means that customers can validate if the business is actually performing the tasks that they say. For example, is your favorite children's cereal company actually buying corn without GMO seeds?

Using a blockchain can result in financial transparency and reduce the need for intermediaries. Other considerable benefits of blockchain solutions in the logistics sector include the following:

- Transparency to the consumers about the supply chain concerns such as farm to table
- Incentives or responsibility from the suppliers to act responsibly and ethically
- Mileage verification for truckers and their drivers to meet the government agency reporting requirements
- Labor verification where no children are used in the mining or processing of jewelry
- Validation of ethical sourcing from suppliers such as fish processors
- An immutable shared view of the ledger that can be viewed by customers of a baby formula manufacturer

NOTE "Dubai's adoption of blockchain technology at a city-wide scale is a testament to its commitment to positively transform government, from service provider to service enabler . . . . We believe blockchain technology, with its built-in efficiency, accountability and security, holds a key to achieving our vision." —Dr. Aisha Bin Bishr, director general at Smart Dubai Office (`https://www.unlock-bc.com/news/2017-12-19/the-transformed-role-of-government-in-the-blockchain-era`)

Blockchain Transaction Basics

Blockchain transactions are processed in somewhat different ways depending on the platform. For example, Bitcoin processes transactions differently from Hyperledger Fabric, which should be expected since the use cases are very different.

The focus of this section is to cover consensus and how transactions work at a generic level. Chapter 4, "Understanding Enterprise Blockchain Consensus," covers specific details around transactions for Ethereum, Hyperledger Fabric, R3 Corda, and Quorum.

Consensus

Consensus is effectively the foundational principle of a blockchain and is how the network nodes come to agreement. All nodes in the blockchain network maintain a copy of the ledger, and each node can source historical transactional data from the network to validate requests.

Consensus, simply put, is a way an "agreement" is reached for the distributed ledger nodes on the network. This agreement effectively states how this will be done and what needs to be verified to be a valid transaction.

This approach to an agreement, especially when considering a permissionless blockchain network, is critical since all nodes on the network need to agree on the validity of a transaction. In a permissioned blockchain, this consensus algorithm can be modified or even manipulated through policies.

For example, in Hyperledger Fabric, which is a permissioned blockchain, we can effectively specify how many nodes (peers) need to approve a request. The number of peers can be a single peer, ten peers, or all the peers.

Consensus (agreement) is reached through the implementation of a consensus mechanism, protocol, method, or algorithm. In reality, a mechanism, method, or algorithm are all referring to the same thing, which is how a distributed ledger platform reaches an agreement.

For the purpose of this book, I will mainly reference the *consensus algorithm* since most blockchain technology vendors seem to have standardized on that approach.

Every blockchain has a different blockchain algorithm that provides specific instructions on how the distributed ledger network comes to an agreement and approves transactions.

Proof of work (PoW), proof of stake (PoS), and many other consensus algorithms will be covered in Chapter 4, "Understanding Enterprise Blockchain Consensus," which discusses consensus algorithms in more detail.

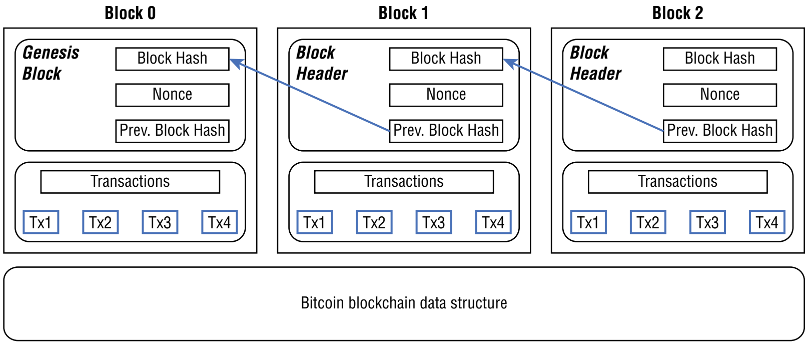
Blocks

Blockchain transactions are recorded on the blockchain network and rely on user verification to be fully authenticated. The transactions executed during a given period of time are recorded into files called *blocks*. Blocks form the foundation of many blockchain networks, as each new block is linked to the previous block of transactions that form the blockchain network.

A transaction is a transfer of cryptocurrency value that is broadcast to the entire network and collected in blocks, as previously mentioned. The recipient of the transaction is represented by the address, which is a string of 26 to 35 letters and numbers. Once verified using the private (secret) key, these transactions are then recorded on the network ledger where this transaction is publicly available. The blocks of transaction information make up the blockchain, with each block's height representing the number of blocks preceding it.

Figure 1.8 shows how a Bitcoin transaction occurs in block sequence. You can trace how block 1 is written first, then block 2 is written, and so on. Note that the hash is referenced in the blockchain, and therefore block 1 would have its hash referenced by block 2, then block 3 would reference block 2's hash, and so on.

FIGURE 1.8 Bitcoin blockchain



Types of Blockchains

Blockchains come in various architectures and can provide for different use cases. Blockchains when appropriately designed will meet the requirements of the enterprise customer and meet the use case required. Enterprises generally prefer blockchains such as Hyperledger Fabric or R3 Corda, which are enterprise focused.

In this section, I will cover blockchain types and deployment concerns and also compare blockchains to cloud computing services.

Public, Private, and Hybrid Blockchains

Blockchains are generally considered infrastructure in most enterprises. *Infrastructure* means that the organization maintains production applications and maintains the application whether directly or indirectly through a service provider.

I generally compare the deployment of blockchains to cloud computing. In cloud computing, there are *deployment models* and *service models*.

A deployment model is essentially a business model. Let's review what NIST states about cloud computing and then let's apply this definition to blockchains.

> *Cloud computing is a relatively new business model in the computing world. According to the official NIST definition, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*
>
> `https://www.bartleby.com/essay/Cloud-Computing-A-Profitable-New-Business-Model-P3S6F9L29BQQ`

The National Institute of Science and Technology (NIST) defines deployment models as follows (`https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf`):

Private Cloud The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers.

Community Cloud The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

Public Cloud The cloud infrastructure is provisioned for open use by the general public.

Hybrid Cloud The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

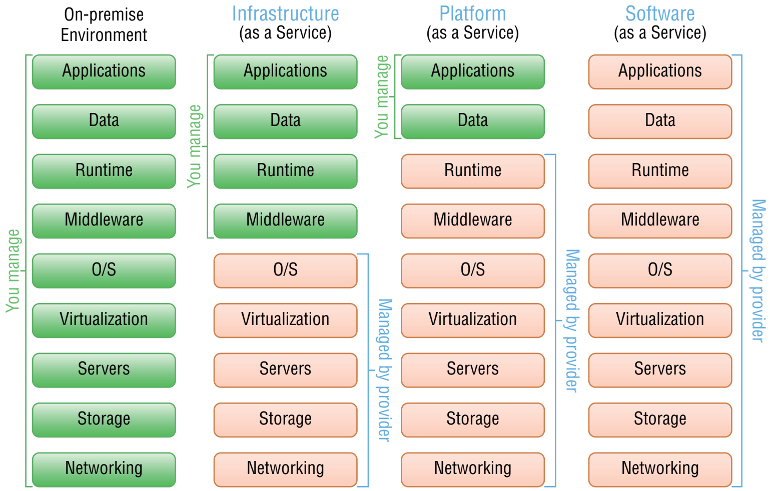
Now if you essentially swap out the term *cloud* with *blockchain*, this is exactly what a blockchain can perform, how it can be deployed, or even how it fits into an enterprise use case.

The notable exception is that in blockchain speak there are no "community" blockchains; however, there are "consortium" blockchains, which are serving the same deployment use case.

These consortium blockchains, which really are "communities," are implemented by like-minded organizations sharing a blockchain. A good example of a consortium blockchain is Ripple, which is used exclusively by the financial industry for interbank payments, for example.

Figure 1.9 illustrates the common cloud computing deployment model. The different service models correlate to the level of effort that is provided by either the provider or the consumer. This model could be used as well for blockchain deployments. For example, blockchains could be deployed in the cloud as a platform or software as a service.

FIGURE 1.9 Cloud computing deployment model



Blockchains are commonly deployed in the cloud and could be deployed as infrastructure/platform/software as a service in a cloud service. Providers such as AWS, Azure, and IBM, for example, provide services that are deployed in all three service models. AWS blockchain templates are considered an IaaS deployment, while IBM Blockchain Platform has two versions: one that is a SaaS and another that is more of a PaaS.

In terms of comparing cloud computing to blockchain, it is important to note that cloud computing at its truest form is a "centralized" approach to computing. Blockchains in their truest form are a "decentralized" form of computing. Anyone who has been in technology understands that when a technology is developed for one use, it generally can be adapted to other use cases. Blockchains are no exception, and as you will read throughout the book, blockchains have many different use cases, exceptions, and variations; some are centralized, and some are decentralized.

For example, Ethereum is essentially a decentralized global computer that processes smart contracts. Ethereum's CTO Gavin Wood describes blockchains as a "global computer." A computer is simply a computational machine; it takes inputs, processes these inputs using certain instructions, and creates outputs.

Blockchains run on computers that are "decentralized" in a permissionless blockchain. In Ethereum, this global computer consists of thousands of nodes that are distributed in more than 100 countries.

NOTE Cloud computing is essentially a business model, and you can choose to deploy that model in several ways. Consider looking at blockchains as a business since they really are just that, a business model. They can be deployed exactly as a cloud computing infrastructure, if that's what the company determines. Private, public, or hybrid deployments are all in use in blockchains today.

Blockchains that are open to anyone are generally considered public, permissionless blockchains. Blockchains that are closed are generally considered private or permissioned blockchains.

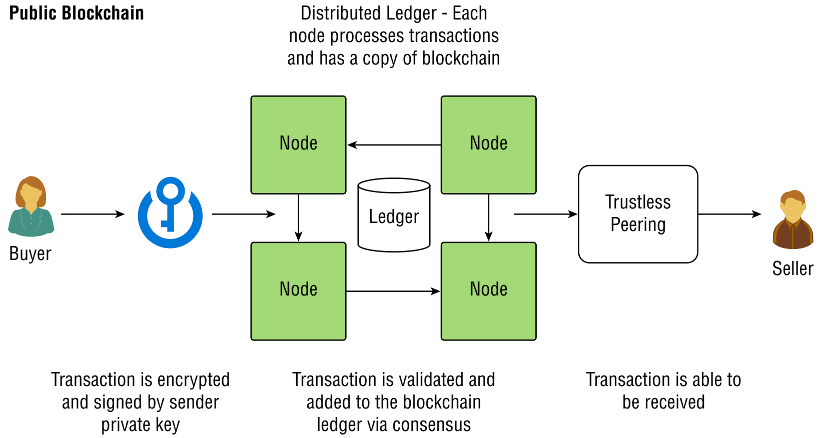
Public Blockchains

Public blockchains are also referred to as permissionless or open blockchains that are open to anyone. Bitcoin was the original permissionless blockchain, as specified and developed by Satoshi Nakamoto. Transactions are processed by all nodes in the blockchain, and those transactions are publicly viewable (transparent) in the blockchain. These transactions are also widely distributed. For example, Ethereum at one time had more than 6,000 nodes worldwide, and each node maintains a copy of every transaction. In Chapter 2, I cover the Ethereum blockchain and its infrastructure in more detail.

Public blockchains are open to anyone, meaning that you can participate in the blockchain. If you want to run an Ethereum node, you simply go to GitHub and download the blockchain. This assumes, of course, that you have the resources to run the blockchain and the technical knowledge to install and configure the blockchain.

Figure 1.10 presents the high-level structure of a permissionless public blockchain and how a trustless peering is imposed on the network—that is, there is no centralized control of membership or participation on the blockchain network.

FIGURE 1.10 Public blockchain example


Public Blockchain
Distributed Ledger - Each node processes transactions and has a copy of blockchain
Buyer
Node
Node
Ledger
Node
Node
Trustless Peering
Seller
Transaction is encrypted and signed by sender private key
Transaction is validated and added to the blockchain ledger via consensus
Transaction is able to be received

Public blockchains have some benefits as compared to private blockchains, as listed here:

- Open read and write
- Widely distributed ledger
- Censorship resistant
- Secure due to mining (51 percent rule)

NOTE Some common public blockchain examples are Bitcoin, Ethereum, and Monero.

Private Blockchains

Private blockchains are also referred to as *permissioned blockchains* or *enterprise blockchains*. These private blockchains are a hybrid of a true blockchain since they are not decentralized but are more centralized. Centralization is at the core of an enterprise blockchain since one entity or a consortium maintain access to the blockchain. Accessing the blockchain network requires permissioning, meaning that one or all transactions are permissioned or authorized to proceed.

These blockchains can be open source, consortium, or privately developed blockchains.

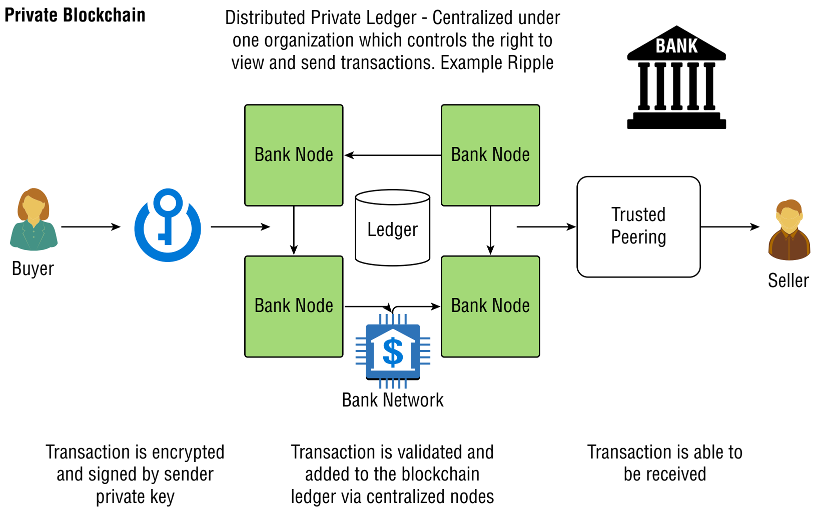
Transactions are also handled differently in a permissionless blockchain. Transactions are processed by select nodes in the blockchain. For example, some blockchains, such as Hyperledger Fabric, can utilize channeling. Channeling can also be used to filter nodes, even in a permissioned blockchain, to keep them from participating in specific transactions that they have no direct interest in.

Transactions are not publicly viewable (transparent) in the blockchain. The transparency of transactions can be permissioned as well. (I will discuss use cases in Chapter 8, “Blockchain Use Cases.”)

The transactions are also generally locally distributed, meaning that the blockchain is in a centrally controlled data center. This approach is essentially the opposite of a permissionless blockchain, where the nodes are processed worldwide on Ethereum blockchain nodes that are in uncontrolled servers.

Figure 1.11 presents the high-level structure of a private blockchain and how a trusted peering is imposed on the network. A private blockchain uses a trusted peering approach, which is different from a public blockchain. The consortium members, for example, will control membership and/or participation on the blockchain network.

FIGURE 1.11 Private blockchain example


Private Blockchain
Distributed Private Ledger - Centralized under one organization which controls the right to view and send transactions. Example Ripple
BANK
Bank Node
Bank Node
Ledger
Bank Node
Bank Node
Trusted Peering
Buyer
Seller
$
Bank Network
Transaction is encrypted and signed by sender private key
Transaction is validated and added to the blockchain ledger via centralized nodes
Transaction is able to be received

Private blockchains have some benefits compared to public blockchains, as listed here:

- They are enterprise permissioned and are controlled for privacy and security.
- They have faster transactions because of fewer nodes and a simple distribution of the nodes such as a limited geography. Node locality and scalability can directly affect performance.
- They have greater scalability because of the configuration flexibility and membership control.
- They have compliance support because of the permissioning and controlled distribution of data storage in appropriate regions.

NOTE Some common enterprise blockchains are Hyperledger, R3 Corda, and Quorum.

Table 1.2 compares the main comparison points of public and private blockchains, including significant differences in security, ledger access, identity, and other features that would be important to consider when designing a blockchain. Private blockchains create value to enterprises through various factors, such as membership, privacy, and even performance.

Table 1.2: Public vs. private blockchains

	Public (Permissionless)	**Private (Permissioned**
Access to ledger	Open read/write	Permissioned read/write
Identity	Anonymous	Known identities
Security and trust	Open network (trust free)	Controlled network (trusted)
Transaction speed	Slower	Faster
Consensus	POW/POS	Proprietary or modular
Open source	Yes	Depends on blockchain
Code upkeep	Public	Consortium or managed
Examples	Ethereum, Multichain	R3 Corda, Quorum

Hybrid Blockchains

A hybrid blockchain is a blockchain that contains the features and functions of both a private, permissioned blockchain and a permissionless blockchain. For example, a company may require intense performance requirements and strict security adherence for their internal employees, but when it comes to B2C transactions, they may place it on an off-chain service (channeling) to process cryptocurrency transactions.

In a nutshell, you may want to consider a hybrid blockchain as similar to a hybrid cloud environment where you take features of both and provide a solution that meets your enterprise's requirements.

Control, performance, transparency, compliance, and other features can be carefully orchestrated in a hybrid blockchain solution. I compare hybrid blockchains to hybrid cloud solutions. A hybrid cloud essentially comprises the best of both worlds in cloud computing.

In a hybrid cloud solution, you can extend our on-premises data center to a cloud computing platform such as AWS. When extended to AWS, your data center can provide many benefits such as cost efficiency by reducing capital expenditures, short time use such bursting services during peak hours, or taking advantage of availability options.

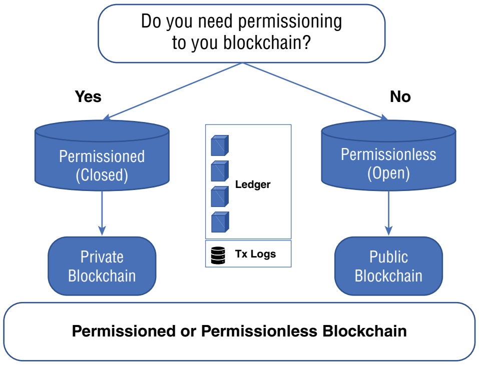
Blockchains when deployed as a hybrid solution can be similar. A company can extend, for example, a Hyperledger Fabric blockchain that is on-premises to AWS or IBM BaaS. The main benefits could be to extend off-chain, to meet compliance requirements, or to extend a blockchain network.

REFERENCE Chapter 7 covers blockchain as a service (BaaS) extensively with step-by-step instructions with AWS Templates and IBM Blockchain.

NOTE "Until now we've seen a proliferation of both public blockchains like Bitcoin and private blockchains like Hyperledger Fabric. Going forward, I think we'll start to see the rise of hybrid blockchains, which combine the best of both worlds." —Stefan Thomas, CTO at Ripple and cocreator of the Interledger payment protocol (`https://bravenewcoin.com/insights/hybrid-blockchains-the-best-of-both-public-and-private`)

Figure 1.12 presents a decision tree for deciding whether to implement a public, private, or hybrid blockchain solution. A hybrid blockchain is an offshoot of a private and permissioned blockchain. A hybrid blockchain can also extend to a permissionless blockchain.

FIGURE 1.12 Blockchain deployment decision tree



When choosing a blockchain type, another factor to consider is cost. I cover the cost of blockchain deployments extensively in Chapter 6, "Enterprise Blockchain Economics."

Large enterprises will generally require the benefits that blockchain technology can deliver without the associated elevated risks of a public blockchain. If this is the case, then a hybrid solution may provide the enterprise with the right solution for the right use case.

In Chapter 3, "Architecting your Enterprise Blockchain," I will discuss how private-public blockchain-focused projects such as Hyperledger, R3 Corda, and Ethereum Enterprise Alliance can enable organizations to be properly scoped around a blockchain solution.

Permissioned or Permissionless Blockchains

In this book, you will notice that *public* and *private* are sometimes used interchangeably with permissioned and permissionless blockchains. To be fair, these terms can in some cases have somewhat different use cases or meanings to different blockchain companies and organizations.

During my years of solutions selling, architecting, and implementing, it's more than fair to say that specific vendors, service providers, and the media make things more difficult than they need to be. Even with the maturity of cloud computing, most vendors add their own twist on top of the industry-wide acceptance of the NIST cloud computing definitions.

Earlier in the chapter I covered public, private, and permissionless blockchain types. Now I'll cover what a permissioned blockchain is. Permissioned blockchains are a form of blockchain that allow only authorized members to join the blockchain. Permissioned blockchains are ideal for enterprises that want some of the benefits of a blockchain such as an immutable ledger but do not want transparency, open membership, or smart contracts. Permissioned blockchains invariably change the initial purpose of what a blockchain originally should be. That is, blockchains originally were open and permissionless, which essentially means they are open to the public.

Summary

Satoshi Nakamoto essentially combined computers and economics to create a blockchain platform called Bitcoin that changed how people needed it to interact with legacy institutions such as banks. Bitcoin came about as a direct result of the financial crisis of 2008.

The blockchain technology is revolutionary, especially for the financial sectors and the logistical sectors. As you learned in this chapter, a blockchain is a type of distributed ledger for maintaining a permanent and tamper-proof record of transactional data.

Enterprises are just starting to understand the potential of blockchains for use in their organizations, for their users, and for their customers, and some have already begun adopting blockchain technology.

There are several definitions and several types of blockchain, depending on who you are talking. Blockchains that are open to anyone are generally considered public or open blockchains. Blockchains that are closed are generally considered private blockchains. Finally, enterprise blockchains are generally private, permissioned blockchains.